Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 08 January 2004

Current Nationwide Threat Level is
HIGH
High Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Atlanta Journal−Constitution reports authorities in Georgia have arrested 53 people and are looking for 27 more who allegedly used the identities of dead people to bolster their credit ratings to buy cars. (See item 6)
- Reuters reports U.S. and Canadian officials said they were trying to track down a second shipment of cattle imported from the same farm where a Washington state cow diagnosed with mad cow disease was born. (See item 16)
- The Register reports Microsoft has released a tool to clean up systems infected by the infamous Blaster worm and its sundry variants. (See item 25)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: High, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *January 07, Dow Jones Business News* — **Energy agency sees demand for oil outpacing forecasts. U.S. and world oil demand will be higher in the first and second quarters than previously forecast, as economic growth heats up and the cost of natural gas, a competing fuel, remains high, the U.S. Energy Information Administration (EIA) said Wednesday, January 7. The EIA sees world and U.S. oil demand growing more than expected in 2004 and sees demand growing further in 2005,** the agency said in its monthly Short−Term Energy

Outlook report on oil markets. The revisions by the EIA, the statistical arm of the Department of Energy, follow similar upward revisions to demand a month ago and point to a growing appetite for oil at a time when the Organization of Petroleum Exporting Countries is worried about a price crash in the second quarter when demand usually shows seasonal weakness. "This anticipated acceleration in growth is due to continued strong economic growth, high natural gas prices, and the continued use of fuel oil as a substitute in electricity production and industrial processes," the EIA wrote. The expected higher demand, combined with supply restraint by OPEC, will keep U.S. commercial petroleum inventories at the low end of their historical range all year and prices high, the EIA said.
Source: http://biz.yahoo.com/djus/040107/1430001103_1.html

2. *January 07, Victor Valley Daily Press (CA)* — **Nuclear waste sent to New Mexico. Nuclear waste shipments previously canceled because of safety concerns will be transportated on Wednesday, January 7, along the original route, officials said. The U.S. Department of Energy will transport plutonium−contaminated garments, tools and other items from the Nevada Test Site to a New Mexico disposal plant on specially modified flatbed trucks.** The medium−level tran−suranic waste, generated during nuclear weapons development, can take thousands of years or more to decay to safe levels, said Ralph Smith, a spokesperson for the Waste Isolation Pilot Plant near Carlsbad, NM. The material will follow a circuitous route spanning 329 miles of California highways, entering the state on Highway 127, traveling south to Interstate 15 at Baker, southwest to Interstate 40 at Barstow, and then east through Needles into Arizona, Smith said. California Highway Patrol (CHP) officers will escort the trucks during their passage through the state, said Tom Marshall, a CHP spokesperson. **Bob Loux, Nevada Nuclear Projects Office chief, said about 1,650 drums of transuranic waste have been stored for decades north of Las Vegas at the Nevada Test Site, awaiting transport to the plant in New Mexico.**
Source: http://www.vvdailypress.com/cgi−bin/newspro/viewnews.cgi?newsid1073499415,98754,

[Return to top]

Chemical Sector

3. *January 07, Associated Press* — **Plant explosions keep dozens from going home.** Dozens of people were kept from their homes Wednesday as firefighters working in freezing temperatures sprayed water on a chemical plant where a series of explosions injured two people and forced thousands to evacuate. **The explosions at Arkansas's Detco Industries plant Tuesday morning shot fireballs into the sky and sent up a plume of smoke so thick it could be seen 30 miles away in Little Rock. Everyone within a mile of the plant was ordered to evacuate.** Wednesday morning, residents were still being kept from trailer homes near the plant, but schools and several businesses in the area reopened. One worker injured in the blast was hospitalized in critical condition; the other was in stable condition in a hospital burn unit. Officials with Detco, which makes industrial chemicals and aerosol products, such as cleaners and disinfectants, said they did not know what caused the explosions. **Federal documents filed by the company show the plant had hydrofluoric acid, sulfuric acid and methanol on the premises,** said Jennifer Gordon, spokeswoman for the Arkansas Department of Emergency Management. The Department of Environmental Quality, which set up portable air monitoring

stations in the area after the explosions, said it did not believe any toxic material was carried to populated areas in the town of 46,000.
Source: http://www.cnn.com/2004/US/South/01/07/plant.explosion.ap/in dex.html

4. *January 07, WXIA TV (Atlanta, GA)* — **Cold air helps curb chemical leak.** The cold temperatures in the Atlanta Metro area help stem a chemical leak that forced the closing of Stewart Road at Buford Highway near the Doraville MARTA station. **Authorities tell 11Alive News that between 40 to 200 gallons of a flammable herbicide leaked onto the street and into a nearby storm drain. Hazardous material and fire crews were on the scene to monitor the situation, fearing the chemical would make its way into Peachtree Creek.** However, because of the cold weather, the chemical quickly froze into a puddle. One nearby restaurant had to close for lunch and some evacuations were considered, officials said.
Source: http://www.11alive.com/news/news_article.aspx?storyid=41280

[Return to top]

Defense Industrial Base Sector

5. *January 06, Govexec.com* — **Pentagon begins to gather base−closing data. The Department of Defense is asking military installations to gather information that it will use in deciding which bases to close in 2005.** In a statement Tuesday, January 6, Pentagon officials said the "data call" is one of many steps in the base realignment and closure process. All installations in the United States and its territories were asked for the same information, such as size and type of facilities, so that all receive equitable treatment, according to the statement. The Pentagon will use the information in making recommendations to an independent, bipartisan panel that will report to Congress on which bases to close. **Secretary of Defense Donald Rumsfeld has said the upcoming round could be larger than all the other rounds combined.** He has earmarked billions of dollars in expected savings from closures for military transformation efforts.
Source: http://www.govexec.com/dailyfed/0104/010604g1.htm

[Return to top]

Banking and Finance Sector

6. *January 07, Atlanta Journal−Constitution (GA)* — **Alleged car scam by identity thieves. Authorities in Georgia arrested 53 people Tuesday, January 6, and were looking for 27 more who allegedly used the identities of dead people to bolster their credit ratings to buy cars.** The Georgia Bureau of Investigation (GBI) said the arrest warrants were executed before dawn Tuesday and targeted 80 people in 11 counties. About 100 cars were purchased in the past five years using identities of dead people in Georgia, California, Oklahoma, Ohio and Virginia, the GBI said. **At the center of the scheme was an Albany, GA, woman, Kwezeta Butler, who would sift through newspaper obituaries for names of people who recently died,** said GBI spokesperson John Bankhead. The deceased had either lived in Georgia or had families who placed obituaries for them in local papers. **Butler then paid an Internet search company for background checks on the names and obtained Social Security numbers, dates of birth**

and credit histories of the deceased, Bankhead said. He said Butler sold the information for $500 to $600 to people with poor credit. They in turn used the information to list the deceased as co−signers on car loan applications, Bankhead said.
Source: http://www.ajc.com/metro/content/metro/0104/07scam.html

[Return to top]

Transportation Sector

7. *January 08, Department of Transportation* — **Federal Railroad Administrator announces $233 million loan to Dakota, Minnesota & Eastern Railroad.** A $233 million federal loan granted Wednesday, January 7, by the Federal Railroad Administration will provide enhanced access to international markets and expanded economic benefits for regional railroad customers in Iowa, Minnesota and South Dakota. The Railroad Rehabilitation and Improvement Financing (RRIF) direct loan was provided to Dakota, Minnesota & Eastern Railroad (DM&E) and its subsidiary Iowa, Chicago & Eastern Railroad (IC&E), both headquartered in Sioux Falls, SD. **U.S. Secretary of Transportation Norman Y. Mineta stressed the vital role of regional railroads in the American economy, "President Bush is committed to growing the economy and the RRIF program provides targeted innovative finance opportunities that yield significant economic benefits."** The DM&E and IC&E serve a large area in eight North Central states and are a major component of the freight transportation systems of Iowa, Minnesota and South Dakota. The DM&E is 1,103−mile regional railroad that currently serves 130 companies. The IC&E is a wholly owned subsidiary of the DM&E that serves approximately 750 companies on a 1,403−mile system.
Source: http://www.dot.gov/affairs/froa0104.htm

8. *January 07, Department of Transportation* — **Test results published on Security Seals.** Electronic seal technology is maturing and may be applied to container security, according to a study released Wednesday, January 7, by the Cargo Handling Cooperative Program (CHCP). **Electronic seals, or e−seals, have been proposed as a way to improve security and track cargo movements worldwide. However, e−seals would likely have to be standardized in order to be widely used, and the study did not find any one type suitable for use as a standard.** The CHCP, a partnership between the Department of Transportation's Maritime Administration and private industry, compared five electronic security seals proposed for use on intermodal freight containers. The study found that the technology will continue to improve, and that it is critical to allow for growth in performance in application to the industry. **The e−seals have container information and can show if the seal has been subjected to tampering. The tested seals can be "read" by direct contact or on a specific radio frequency, which varies with the type of seal. For a system using e−seals to be efficient, seals would likely have to be "read" by one kind of reader, using one standard radio frequency.** "For e−seals to be useful, there will have to be an accepted international standard," said Maritime Administrator Captain William G. Schubert.
Source: http://www.dot.gov/affairs/MARAD0104.htm

9. *January 07, Associated Press* — **Northwest Airlines to open Portland−Tokyo route.** Northwest Airlines announced Wednesday, January 7, it will open a daily route between Portland and Tokyo in June, restoring passenger service between Oregon and Asia. The city

lost its only international passenger flight and its last direct route to Asia in March 2001 when Delta Airlines canceled service from Portland to Japan. But business and government leaders have pushed hard to restore international air service, succeeding in October 2002 when Lufthansa announced it would offer service between Portland and Frankfurt, Germany. The Lufthansa flights began in March 2003, the same month that Mexicana Airlines announced it would offer daily passenger service to Guadalajara, Mexico. The service began last May. **The new service will make Portland the airline's eighth U.S. port from Japan and its fourth West Coast link with Tokyo, more than any other airline, Northwest officials said.** The airline said the decision came after Oregon business and government leaders promised the flight would have strong support.
Source: http://www.miami.com/mld/miamiherald/business/7653756.htm

10. *January 07, Associated Press* — **Some I−80 traffic restored after 50−vehicle crash that killed four.** Workers were able to open one eastbound lane of Interstate 80 Wednesday, but westbound lanes remained closed a day after a 50−vehicle crash that killed four people. Mike Hoy, safety spokesman for the Pennsylvania Department of Transportation's Clearfield office, said a single eastbound lane was opened at about noon Wednesday, although traffic at the bottleneck remained backed up. About 30 tractor trailers and 20 passenger vehicles were caught up in a chain−reaction crash near the Bellefonte exit late Tuesday morning, January 6, when a snow squall caused a blinding whiteout. Four people were killed and more than a dozen injured in the larger crash, and fire crews worked into the night to put out a stubborn fire that consumed several vehicles. **Cleanup efforts were delayed Wednesday morning when hydrochloric acid that had been repackaged at the crash site began to breech the new containers, forcing workers to recall hazardous materials crews. Troopers had warned Tuesday that some of the trucks in the crash may have carried hazardous materials, and the Bald Eagle State Park was closed after the crash as a precaution.**
Source: http://pennlive.com/newsflash/pa/index.ssf?/base/news−11/107 3508845217370.xml

11. *January 07, Associated Press* — **Bridge closed twice after security threat.** Erring on the side of caution, law enforcement officials shut down Maine's four−lane Casco Bay Bridge twice Wednesday following a threat overheard on a marine radio channel. **The bridge was shut down for five hours following the threat at 12:28 p.m. and then again for 30 minutes in the afternoon because the threat specifically mentioned something happening at 12:59 p.m. The radio message intercepted by the Coast Guard featured a woman's voice talking about the destruction of the bridge, officials said.** FBI Special Agent James Osterreider said law enforcement agencies decided to err on the side of caution even though the FBI officials who reviewed the tape said they were leaning toward declaring it a hoax. **During the second shutdown, camouflage−clad officers equipped with automatic weapons patrolled the bridge on foot while uniformed police officers and a bomb−sniffing dog swept the area under the bridge.** Air traffic was shut down and a Coast Guard helicopter hovered overhead. Coast Guard vessels also patrolled the waters. Officials conducted a thorough search of the bridge overnight but found nothing suspicious. It was reopened around 6 a.m., in time for the busy morning commute.
Source: http://news.mainetoday.com/apwire/D7VU6AVO0−6.shtml

12. *January 07, Braintree Forum (MA)* — **Suspicious devices close Fore River Bridge twice. The first incident occurred New Year's Eve at about 4 p.m. when the Quincy, MA, Police**

marine unit spotted what appeared to be two bags suspended from ropes underneath the bridge. The Coast Guard was notified and sent a unit from the Point Allerton station in Hull. Both Weymouth and Quincy police responded and shutdown the bridge to traffic while Coast Guard officials investigated the suspicious items. Just before 6:30 p.m., the bridge was reopened after it was determined the devices were actually buoys used by Middlesex Construction Company to mark underground cables in the Fore River when the old bridge is dismantled. **The second incident happened Saturday, January 3, at about 12:20 p.m. According to Deputy Fire Chief Joseph Davis, Weymouth police received a call over their business line that there was a bomb on the bridge.** Davis responded along with Engine 1 and set up a staging area in a parking lot across from Bluff Road while police closed off the bridge to traffic. A thorough search turned up nothing and the bridge was reopened to traffic at about 1:30 p.m. Patrols of the Fore River Basin have been stepped up since Homeland Security placed the country on orange alert. Within the basin are the Fore River Bridge, the Exelon Power plant, Twin Rivers Technologies, the Citgo fuel farm, and the MWRA fertilizer plant.
Source: http://www.townonline.com/braintree/news/local_regional/bra_newwntombridgeclose01072004.htm

[Return to top]

Postal and Shipping Sector

13. *January 07, DM News* — **USPS: Letters, cards up for holidays. Seventy−eight million more letters and cards were postmarked this holiday season versus last year, postmaster general John E. Potter told the U.S. Postal Service's Board of Governors Tuesday at its monthly meeting.** A record 3.4 billion cards and letters were postmarked December 1−24. Postmarks on December 22 rose 25 percent over last year. From Thanksgiving to Christmas the USPS handled more than 20 billion pieces of mail. On the busiest day, December 15, more than 850 million pieces entered the postal system. December 17 was the year's busiest delivery day, with about one billion pieces. The more than 24 million pounds of holiday mail to the Persian Gulf and other military locations worldwide surpassed last year's volume by 11 million pounds, or almost 85 percent. The need for additional holiday hires was reduced to about 13,000 from last year's 20,000 thanks to advances in mail−processing technology. High−speed sorting equipment can process nearly 80 percent of all handwritten addressed mail.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=2609 9

[Return to top]

Agriculture Sector

14. *January 07, USAgNet* — **Chickens dead from virus in Vietnam. Vietnamese Agriculture officials met to work out measures to contain transmission of a mystery virus that has killed as many as 60,000 chickens in southern Vietnam.** The disease first emerged last week in the southern provinces of Tien Giang and Long An but has subsequently spread to other Mekong Delta provinces and Ho Chi Minh City as a result of panic selling by local farmers. Around 1,600 kilograms of chickens felled by the virus have been buried in specially dug pits in Ho Chi Minh City over the last few days, and city authorities have banned import of

chickens from Tien Giang and Long An. Agriculture inspectors have been deployed to local markets in the southern business capital and the two provinces to monitor poultry sales and to seize and destroy all dead chickens. "We estimate that eight to 10 percent of around 600,000 chickens that have been sold have died," said Nguyen Van Hung, an official from the Long An provincial government's veterinary department. **Vietnam does not export any chickens.**
Source: http://www.usagnet.com/story−national.cfm?Id=19&yr=2004

15. *January 07, Ohio Ag Connection* — **Prion test would allow early detection TSEs. Ohio State University researcher Srinand Sreevatsan is creating tools to detect mad cow disease.** "There is a desperate need for a fast and reliable test for the diagnosis of transmissible spongiform encephalopathies (TSEs) in live animals," said Sreevatsan. **"Early detection could lead to efficient surveillance systems that may avert or control this group of diseases."** Funded by a three−year U.S. Department of Defense grant, Sreevatsan is developing a test to detect prions, the agents responsible for bovine spongiform encephalopathy (BSE, commonly known as mad cow disease) and other TSEs such as scrapie in sheep and goats, chronic wasting disease in deer and elk, and Creutzfeldt−Jakob disease in humans. **Currently, definite diagnosis of TSEs is only possible after death, which limits surveillance efforts.** Sreevatsan's lab is looking for a way to identify prions through clinical samples such as blood, serum, or lymphoid tissues before the onset of symptoms. **"The idea is to detect the prion protein, which is folded abnormally as compared to its normal counterpart, in an animal that's still living, using non−invasive approaches," Sreevatsan explained.**
Source: http://www.ohioagconnection.com/story−state.cfm?Id=5&yr=2004

16. *January 06, Reuters* — **Mad cow probe finds more cattle sent to U.S. U.S. and Canadian officials on Tuesday said they were trying to track down a second shipment of cattle imported from the same farm where a Washington state cow diagnosed with mad cow disease was born.** The infected cow and 80 or 81 other cattle from a Canadian herd crossed into the United States in September 2001. "A subsequent group of 17 younger animals from the farm were held back for a period of time," Brian Evans, Canada's chief veterinarian, told reporters in a joint news conference with USDA. **"Some of the animals were bred and then moved into the U.S. in a second wave of export."** Evans also said a number of calves from the herd remained in Canada and were currently under quarantine. Officials said there was no evidence that mad cow disease had spread to the other cattle. **USDA spokesperson Julie Quick said the department was "still not sure" whether the second shipment of cattle actually entered the United States.** "We are looking at records," she said. "If they did enter the U.S., we will trace them here. If they are in Canada, they will be traced by Canada." Quick said there was a possibility that there may be more cattle from the birth herd in Alberta that need to be located.
Source: http://www.agriculture.com/worldwide/IDS/2004−01−06T231735Z_01_N06293854_RTRIDST_0_MADCOW−HERD−UPDATE−1.html

[Return to top]

Food Sector

17. *January 06, Reuters* — **Canada, U.S. to discuss feed rules this week.** Canadian and U.S. officials will discuss the possibility of instituting stricter rules on what goes into livestock feed

after two recent cases of mad cow disease in North America, Canada's farm minister said on Tuesday. **Two animal health officials from the Canadian Food Inspection Agency will meet with counterparts in Washington on Thursday to talk about whether cattle brains, spines and other materials thought to spread mad cow disease should be removed from all livestock feed, Agriculture Minister Bob Speller told reporters at a news conference.** Canada banned the risk materials from the human food chain in July, following an international review of the way it handled its first home−grown case of mad cow disease in May. That safety measure was mirrored by the United States after it found a diseased cow last month in Washington state. The international panel also recommended Canada ban the materials from animal feed, which Canadian officials have since pondered. Strengthening feed rules could add costs, Evans noted. **"There are broader implications in terms of the environmental disposal of that material, alternate uses for those materials, and ensuring the measures being taken would be enforceable," he said.**
Source: http://www.agriculture.com/worldwide/IDS/2004−01−06T224522Z_01_N06297772_RTRIDST_0_MADCOW−CANADA−FEED.html

[Return to top]

Water Sector

18. *January 06, American Chemical Society* — **MTBE alternatives could pose similar environmental threat.** New research suggests that expanded use of MTBE alternatives may pose as much of an environmental threat as their predecessor. **The solution, the researchers say, is to stop fuel tank leaks before they start by designing better storage tanks.** Bans on the use of MTBE are scheduled to go into effect January 1 in California, Connecticut, and New York. Seventeen other states, are considering restrictions or bans on MTBE, **citing concerns that it can leak from gasoline storage tanks and contaminate drinking water supplies. The researchers analyzed data from groundwater samples taken at 868 leaking fuel tanks in Los Angeles, CA, measuring the concentration of each oxygenate.** The 1990 Clean Air Act Amendments require that gasoline formulations contain oxygen to help them burn more completely. Tom Shih, an environmental scientist with the California Environmental Protection Agency and his colleagues investigated the extent of groundwater contamination beneath gas stations, automotive shops, and other sites with leaking underground fuel tanks in the Los Angeles area. **The study focused on MTBE and four other additives with similar properties. "All indications suggest that the alternative oxygenates would pose groundwater contamination threats similar to MTBE if their scales of usage were expanded,"** the researchers conclude.
Source: http://www.innovations−report.com/html/reports/environment_sciences/report−24495.html

[Return to top]

Public Health Sector

19. *January 07, University of California, San Diego* — **Insight into anthrax evasion of host's immune response.** Biologists at the University of California, San Diego (UCSD) have

determined how toxin produced by anthrax bacteria blocks a person's normal immune response. **The UCSD scientists found why human immune cells fail to respond normally to lipopolysaccharide, a component of the cell walls of Bacillus anthracis.** Bacterial invasion, or the presence of lipopolysaccharide, usually causes immune cells known as macrophages to release cytokines. Release of cytokines causes large numbers of immune cells to arrive at the site of infection and destroy the bacteria. It turns out that there are two separate routes in the cell by which a series of proteins activate one another to switch on production of cytokines. One of the routes has been known. The scientists identified the second route, the IRF3 pathway. The anthrax toxin targets the IRF3 pathway by cleaving MKK6, one of the proteins along the route. The cleavage of MKK6 prevents the cytokine genes from being switched on. **This suggests that developing a drug that could protect MKK6 and prevent anthrax toxin from cleaving it could help to prevent an anthrax infection from getting out of control. The anthrax bacteria would be unable to evade the normal immune response.**
Source: http://www.sciencedaily.com/releases/2004/01/040107072134.ht m

20. *January 07, Independent − UK* — **Vaccine may offer full protection from meningitis. A vaccine that could provide protection against every strain of meningitis is being developed by British scientists. Although vaccines already exist for the A and C strains of meningitis, it is the first time researchers have successfully created a shot which can protect against meningitis B, the most dangerous form of the disease.** Meningitis B is the most common strain of the disease in Great Britain, accounting for 60 percent of cases. Around 3,000 people are infected every year, and 200 die as a result of the disease. Many survivors are left severely handicapped. Meningitis A is seldom seen in the UK, but is a much bigger problem in other parts of the world. Meningitis C was once the most common strain in Great Britain, accounting for 40 percent of cases in 1998 and killing hundreds of children each year. But the introduction of a widespread vaccination program in 2000 has virtually wiped out the disease, with deaths falling to single figures. Meningitis B has proved harder to create a vaccine for because there are many different strains circulating. **Other teams have been working on a meningitis B vaccine, but this is the first to target all three strains. It could be a very powerful tool in the eradication of meningitis.**
Source: http://news.independent.co.uk/uk/health/story.jsp?story=4787 81

21. *January 07, Guardian − UK* — **NHS receives new virus and terrorism guidance.** New guidance for the UK National Health Service (NHS) on planning for emergencies and major incidents has been issued by the health secretary, John Reid. **The document, Handling Major Incidents: An Operational Doctrine, builds on current guidance by setting out general principles to help the NHS develop its existing emergency plans to respond to new potential threats.** The paper also reflects structural and organizational changes in the NHS over the past few years. "The NHS has always been ready to cope with major incidents, and over the past half−century has repeatedly proved itself up to the task. But we must recognize we live in a constantly changing world, where new potential threats have emerged," said Reid. "These may be natural, for instance previously unrecognized viruses, or man−made, in the shape of terrorism. The NHS has already responded to these changing circumstances by revising and improving its planning. Today's guidance will provide further help and ensure the entire service is able to work together smoothly if needed."
Source: http://politics.guardian.co.uk/attacks/story/0,1320,1117984, 00.html

22. *January 06, Associated Press* — **CDC warns flu season still hasn't peaked.** The flu season has yet to reach its peak, despite a drop−off in cases in some states, health officials warned on Tuesday. At least five states, Kansas, Kentucky, Nebraska, Washington, and West Virginia, no longer have widespread outbreaks of flu, but 42 others still do, the U.S. Centers for Disease Control and Prevention (CDC) said. **"If you look at overall data from nationwide surveillance, it doesn't look like it's peaked yet," said Scott Harper, a CDC flu expert. "Nationwide, influenza−like illnesses are still on the rise."** Nationally, more people are visiting the doctor for flu−like illnesses. About 9.4 percent of all outpatient visits surveyed by the federal agency last week involved flu−like illnesses, up from 7.7 percent in the previous week and the highest rate so far this season. In addition, pneumonia and influenza accounted for a season−high nine percent of deaths, up from 7.8 percent the previous week, in a survey of 122 U.S. cities.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=541&ncid=718&e=10&u=/ap/20040106/ap_on_he_me/flu_season_cdc

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

23. *January 07, Firehouse.com* — **Colorado's 911 backup system not working. The 7NEWS investigators have learned that Denver's 911 backup system isn't working at a time when our nation's homeland security remains on high alert. The city's main 911 call system is operating without any problems but the concern is that if that system fails for any reason, the city is without a backup.** It's like a high−wire circus act performing without a net, Investigator Tony Kovaleski said. "I think we're concerned because if we have an incident that occurs at the primary communications center, we need somewhere to go to transfer those emergency calls to," said Tracy Howard, the director of Department of Public Safety. The emergency backup plan should immediately transfer all 911 and non−emergency calls from the main facility to the city's emergency management center in the basement of the city and county building. But during its fourth consecutive test in three months, the backup system failed. Denver's Public Safety Department scheduled a high level meeting with Qwest for Monday to get to the bottom of the problem. The city expects to resolve the problem by the end of next week but for now the city's emergency call center is online without a safety net.
Source: http://cms.firehouse.com/content/article/article.jsp?id=sect ionId=46&id=24085

24. *January 07, McCook Daily Gazette (NE)* — **Heineman: Other states admire Nebraska's efforts on Homeland Security.** "Nebraska has a national reputation for its Homeland Security efforts," Nebraska's lieutenant governor Dave Heineman told McCook and Red Willow County law emergency response providers Tuesday morning, January 6. **Heineman praised what he and other Homeland Security officials are calling "The Nebraska Model" −− where all responders know and understand the capabilities and responsibilities of each department,**

and "all departments focus on one mission." Lt. Gov. Heineman, who is also the state's director of Homeland Security, visited with emergency responders about how they are spending federal funds allocated for Homeland Security efforts. "We want to get a good sense of local−level Homeland Security efforts," Heineman said, "and how the money is being spent. We're allowing local units to determine the use of the money, because that's the way it works best." Bud Keenportz, coordinator of Red Willow county's Local Emergency Planning Committee, told Heineman he would like to create exercises on mad cow disease response, a hazardous materials incident and a hostage situation.
Source: http://www.mccookgazette.com/story/1059243.html

[Return to top]

Information and Telecommunications Sector

25. *January 07, Register* — **Microsoft releases Blaster clean−up tool. Microsoft this week released a tool to clean up systems infected by the infamous Blaster worm and its sundry variants. The software should eradicate the worm from infected Windows XP and Windows 2000 machines. However, users will still have to apply the original patch to prevent re−infection**. Normally, such clean−up technology is left to antivirus firms. But this isn't a normal viral epidemic: **ISPs say the worm is still generating malicious traffic, months after its first appearance**. Microsoft's Windows Blaster Worm Removal Tool will disinfect machines infected with either the Blaster or Nachi worms. Nachi, released shortly after the first appearance of Blaster in August, was designed to patch vulnerable systems. Rather than help out, Nachi has instead become a serious nuisance. Its aggressive scanning behavior blighted the operation of many networks − hence the need to kill the "cure", along with the original Blaster worm. The tool is available at
http://www.microsoft.com/downloads/details.aspx?FamilyID=e70a0d8b−fe98−493f−ad76−bf673a38b4cf&displaylang=en
Source: http://www.theregister.co.uk/content/56/34751.html

26. *January 06, esecurityplanet.com* — **Trojan sends spammed message with woman's picture. BackDoor−AWQ.b is a remote access Trojan** written in Borland Delphi, according to McAfee, which issued an alert Tuesday, January 6. **An email message constructed to download and execute the Trojan is known to have been spammed to users. The spammed message is constructed in HTML format. It is likely to have a random subject line, and its body is likely to bear a head portrait of a lady** (loaded from a remote server upon viewing the message). The body contains HTML tags to load a second file from a remote server. This file is MIME, and contains the remote access Trojan (base64 encoded). Upon execution, the Trojan installs itself into the %SysDir% directory as GRAYPIGEON.EXE. A DLL file is extracted and also copied to this directory (where %Sysdir% is the Windows System directory, for example C:\WINNT\SYSTEM32) The following Registry key is added to hook system startup: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion \RunOnce "ScanRegedit" = "%SysDir%\GRAYPIGEON.EXE" The DLL file (which contains the backdoor functionality) is injected into the EXPLORER.EXE process on the victim machine. More information, including removal instructions, can be found
at:http://us.mcafee.com/virusInfo/default.asp?id=description &virus_k=100938
Source: http://www.esecurityplanet.com/alerts/article.php/3295891

27. *January 05, esecurityplanet.com* — **Multi−component worm searches for weak system passwords. Sophos issued a low−level alert for W32/Randon−AB, a multi−component network worm that attempts to spread by copying components of itself to and executing them on remote ADMIN$ shares with weak passwords**, on Monday, January 5. One component of the worm, B4AK.EXE, then attempts to download and execute a copy of the worm from a remote URL as a file called C:\SVCHOST.EXE. The main file is an SFX EXE which creates a folder called AL within the Windows system folder and drops and executes several files, some of which are legitimate utilities or innocuous files. The worm adds an entry to the registry Run Key to run H00D.EXE on system restart. **Instructions for removing worms are at** http://www.sophos.com/virusinfo/analyses/w32randonab.htm l
Source: http://www.esecurityplanet.com/alerts/article.php/3295121

28. *January 05, eweek.com* — **Agencies beef up IT security.** The Department of Justice (DOJ), one of a handful of agencies that received a failing grade on last month's report card on IT security delivered by a congressional subcommittee, is at the forefront of the movement. **The DOJ has made a number of changes, including the establishment of a department−wide IT security staff that answers directly to the CIO**, according to DOJ officials. That group, in turn, has set about organizing a security council within the department, they said. The council comprises the top security officials from each of Justice's dozens of component organizations, and is now responsible for implementing and overseeing all the security programs in the department. So far, the results have been encouraging, department officials said. Another agency, **the Environmental Protection Agency has created an automated security evaluation and remediation application capable of testing the security posture of each machine and monitoring the remediation process for any problems found. The Department of Transportation recently implemented a comprehensive vulnerability assessment and remediation package** that performs continuous scans, instead of the traditional monthly or quarterly assessments.
Source: http://www.eweek.com/article2/0,4149,1426312,00.asp

Internet Alert Dashboard

Current Alert Levels

AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.G** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	

	901 (realsecure), 6129 (dameware), 135 (epmap), 1434 (ms−sql−m), 137 (netbios−ns), 139 (netbios−ssn), 23 (telnet), 21 (ftp), 445 (microsoft−ds), 27374 (SubSeven) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

29. *January 07, CNN* — **French seek man from canceled flight. French authorities said Wednesday they are looking for a man, believed to be an Afghan, who failed to show for an Air France flight to the United States that was canceled for security concerns.** The French Interior Ministry National Police said the man was booked on Air France Flight 68 from Paris to Los Angeles, California, on December 24, one of six Air France flights between the two cities canceled on December 24 and 25. **The man, Abdul Hay, has the same name as an Afghan who escaped U.S. custody in Khandahar, Afghanistan, the French intelligence sources said.** Abdul Hay was known to be close to former Taliban chief of intelligence Mullah Mohammed Abdul Haq, the sources said. **French and U.S. authorities do not know whether the Abdul Hay who booked a seat on the Air France flight is the same man.** French Justice Minister Dominique Perben, in a radio interview Wednesday with Paris−based Radio Monte Carlo, said, "I confirm that we are looking for someone, but I can't say more. What's important when someone doesn't take a plane is to know why he didn't take it."
Source: http://www.cnn.com/2004/US/01/07/terrorism.threat/

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer